

U.S. EUROPEAN COMMAND

Host Commander Site

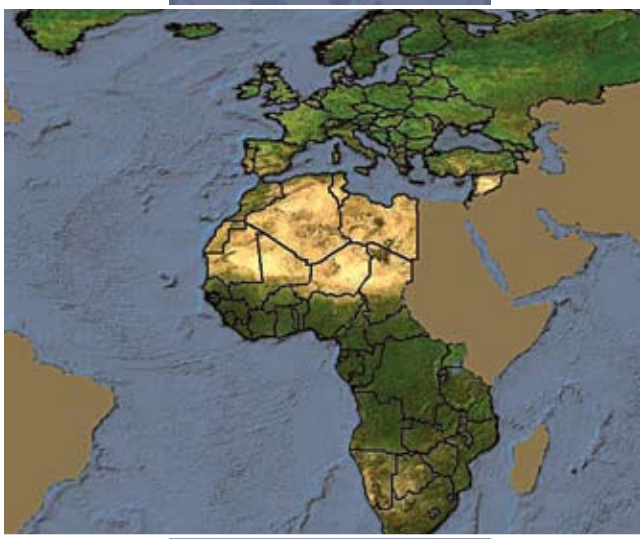
U.S. European Command (USEUCOM) is the unified combatant command charged with defending and advancing US national interests in a 92-country area of responsibility spanning from the North Atlantic east across Europe to Russia, and south from the north pole to South Africa.

Diverse is the word which best describes EUCOM's theater, which includes many of the world's richest and poorest nations. The command maintains ready forces to conduct the full range of operations, unilaterally or in concert with coalition partners, to promote regional stability, counter terrorism and enhance transatlantic security through support of NATO. EUCOM is transforming its base and force structure to become more agile, expeditionary, capable and interoperable – all essential to meeting the challenges of today's complex security environment.

The command strategy emphasizes preventive, "Phase 0" theater security cooperation. This approach seeks partnerships to enhance regional security capabilities in developing nations, denies safe haven for terrorists and deals with underlying causes of conflict. Building on the strength of a transformed NATO alliance and working with key countries and regional organizations in Africa, Eastern Europe and the Caucasus are key elements of this strategy. Equally important is establishing command and control structures and processes that take advantage of new technologies, leverage the capabilities of the inter-agency community, and enable faster, flexible planning and execution with effects-based solutions.

Coalition interoperability is absolutely critical if we are to rapidly respond to events that may occur with little or no warning. This year's Coalition Warrior Interoperability Demonstration (CWID) will help close the gaps by evaluating trial technologies that demonstrate warfighter utility and can be fielded within 12-18 months.

EUCOM is proud to be the host combatant command for CWID 2007 and 2008. This year's demonstrations will be hosted at Kelley Barracks in Stuttgart, Germany, from June 4 until June 22, 2007.



SCHEDULE OF EVENTS

May 29-June 21: Execution

- **May 29-June 1:** National Integration/Final Testing and Trial Set-Up
- **June 4-8:** Coalition Integration, Scenario Training and Rehearsal
- **June 11-15:** Execution and Assessment
- **June 18-21:** Visitor Week
- **June 22:** Hot Wash

TRANSPORTATION INFORMATION AND DIRECTIONS

FROM THE STUTTGART AIRPORT TO KELLEY BARRACKS

- **A taxi from the airport** to Kelley Barracks is about 15 Euros ($18). Although some taxis will take credit cards, the best bet is to use the airport ATM or currency exchange before leaving the airport so you can pay in cash. You can request a KreditKarte (Credit Card) taxi from the queue. The drivers provide receipts upon request. Tipping is not necessary but is appreciated. 1-2 Euros is sufficient.
- **Driving from airport exit,** turn left. Stay in the right lane looking for Route 27 towards Stuttgart, approximately .5 miles. Stay in right lane to get on Route 27 and then move to the center lane.
- Once you have passed the exit for A8, stay to the right for about 1.5 miles. You will go one more exit before getting off. Follow signs for Kelley Barracks. Keep right and make the right hand turn, then change to the left lane. Pass the first light and turn left at the second light.
- Stay to the left after making the turn. Kelley Barracks starts right after the Daimler-Chrysler complex.
- The gate guard will ask to see your identification (passport or ID card) before permitting you access to the base.

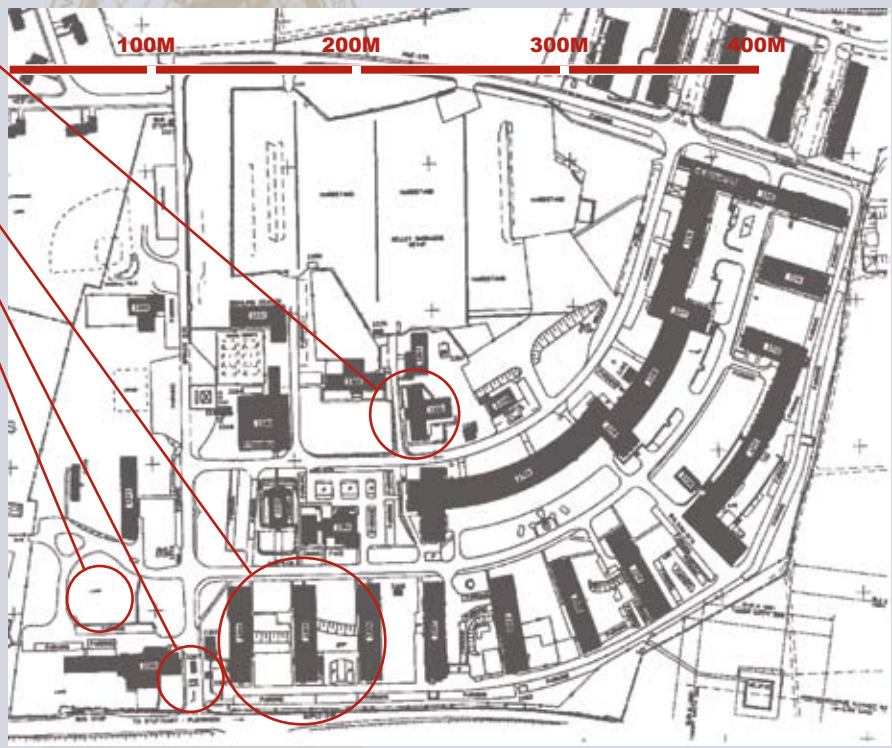
STUTTGART

USEUCOM CWID OPERATIONS BUILDING 3350

BARRACKS

MAIN GATE

KELLEY HOTEL



VISITOR CLEARANCES/BERTHING

Clearances are due to IS2 Shawn Williams no later than May 15, 2007. Badges will be issued for the CWID work site. Please contact CDR Greg Stephens to verify you are listed as a visitor. For government berthing and local assistance, please contact CDR Stephens.

POINTS OF CONTACT

e-mail: cwid@eucom.mil

CDR Greg Stephens
stepheng@eucom.mil

OS1 Roger Nelan
nelanr@eucom.mil

IS2 Shawn Williams
williash@eucom.mil

OTHER PHONE NUMBERS

Kelley Hotel
CML +49 (0)711-729-2815/2304/
DSN 314-421- 2815/2304

USO
CML +49 (0)711-680-5559/DSN
314-430-5559

SI Centrum/Millenium CML +49 (0)711-721-0 (hotel and entertainment complex)

Enjoy Tours
CML +49(0)6301-6000
www.enjoytours.com

Trials at USEUCOM CWID Operations Building

TRIAL NO.	SYSTEM TITLE (ACRONYM OR SHORT NAME)	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	TRIAL SECTION PAGE NO.
1.01	Compartmented High Assurance Information Network (CHAIN)	USNORTHCOM	Raytheon	3
1.17	Cross Domain Collaborative Information Environment/Collaboration Gateway (CDCIE/CG)	US Air Force, USJFCOM, FBI	Trident Systems	4
1.54	Collaborate-Access-Browse (CAB)	NSA	Essex Corporation	5
1.55	Assured File Transfer (AFT)	NSA	CTC, Essex Corp., Tresys Technology	6
3.09	Global Personnel Recovery System (GPRS)	USJFCOM	Innovative Solutions International	12
3.14	Coalition Secure Management and Operations System (COSMOS)	DISA	Booz Allen Hamilton	12
3.31	Coalition Infrared Data Processing (CIDP)	US Air Force	Space and Missile Center, Missile Defense Agency	14
3.39	Command, Control, Communication, Computers and Intelligence Defense Defense (C4I Defense)	Italy	SELEX-SI SpA	15
3.70	Coalition open Joint Operations Picture (CoJOP)	UK	Fujitsu Services	17
3.71	MobiKEY Identity Based Access Drive (MobiKEY IBAD) and Defense Identity Management Network (DEFIMNET)	Canada	Route1, Inc.	17
3.80	Riverbed Information Optimization System (RIOS)	US Air Force, DISA	C2I Solutions, Riverbed	18
6.53	Weapons of Mass Destruction Collaborative Advisory Response System (WMD CARS)	USNORTHCOM	DTRA	24
6.74	Security Information Management for Enclave Networks (SIMEN)	US Air Force	The MITRE Corporation	25

NORTH AMERICAN AEROSPACE DEFENSE - U.S. NORTHERN COMMAND

Site for Homeland Security and Homeland Defense

NORAD-USNORTHCOM, Colorado Springs, Colo., employs CWID to forge new coalitions. Traditional CWID participation expands this year to involve partners in other government agencies that would be part of any emergency response effort.

Future coalitions will be created on the fly, based on events. It will benefit all potential contributors, international and domestic, to be familiar with the military information environment. Many information technologies, along with associated tactics, techniques and procedures to support response efforts, will be evaluated during CWID 2007.

Trials at NORAD-USNORTHCOM will focus on the Homeland Defense mission, demonstrating technological advances in information sharing, collaboration, wireless technologies and web based situational awareness tools.

CWID demonstrations will be hosted at the Federal Building, 1520 E. Willamette, Colorado Springs, Colo., during the execution phase 11 to 21 June, 2007.

Colorado Springs is the second largest city in the state with a population of approximately 500,000. Colorado Springs hosts

CONTACTS

Chris Lambert, Program Manager
719.554.8064, DSN: 692.8064
christopher.lambert@northcom.mil

Annette Guerrero, Site Manager
719.554.2802, DSN: 692.2802
annette.guerrero@northcom.mil

Bill Crimmel, Scenario Lead
719.554.7189; DSN 692.7189
william.crimmel.ctr@northcom.mil

Rex Scifres, Network Engineer and Security
719.554.2873, DSN 692.2873
rex.scifres.ctr@northcom.mil

the United States Air Force Academy to the north, Peterson Air Force Base to the east, Fort Carson to the south, and Schriever AFB to the east. Peterson AFB is home to NORAD-USNORTHCOM. The Federal Building, the CWID 2007 site in the city of Colorado Springs, is an off-base facility. The Colorado Springs Airport, which shares runways with Peterson AFB, services the area with direct connections to many major travel hubs.

FROM THE AIRPORT

Exit the airport via Drennan Road, go west to Powers Blvd.; go north on Powers Blvd to Platte Ave.; go west on Platte Ave. to Boulder; go west on Boulder to Hancock; go north on Hancock to Willamette; go east to 1520 E. Willamette.

SYSTEM ADMINISTRATOR/ NETWORK SECURITY

Sara Wright
719.554.2889, DSN: 692.2889

PUBLIC AFFAIRS CONTACT

LCDR Sean Kelly
719.554.9670
DSN: 834-9670

NORTHCOM OMB

nnc.cwid.omb

CWID Trials at NORAD-USNORTHCOM

TRIAL NO.	SYSTEM TITLE (ACRONYM OR SHORT NAME)	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	TRIAL SECTION PAGE NO.
1.01	Compartmented High Assurance Information Network (CHAIN)	USNORTHCOM	Raytheon	3
1.28	NET/X eToken Security System, Deployable Communications System (NET/X)	USJFCOM	FED-COMM USA, Inc.	4
1.55	Assured File Transfer (AFT)	NSA	CTC, Essex Corp., Tresys Technology	6
1.63	Coalition Assured Sharing Environment (CASE)	DISA	General Dynamics	7
1.86	Federated Identity Management System (FIDMS)	USJFCOM	BearingPoint, Hewlett Packard	8
2.16	Deployable Geospatial Database (DGDB)	Canada	Canada	9
2.21	Commercial Joint Mapping Toolkit (CJMTK)	NGA	Northrop Grumman Corp.	10
2.57	Automatic Ingest, Mosaic and Mapping System (AIMM)	Canada	PCI Geomatics	11
3.09	Global Personnel Recovery System (GPRS)	USJFCOM	Innovative Solutions International	12
3.27	Integrated Information Management System (IIMS)	US Army, US Air Force	US Army, US Air Force	13
3.38	Collaborative Decision Aid (CDA)	USNRTHCOM	ARINC Engineering Services, LLC	15
3.58	US Coast Guard Information Sharing and Communications (USCG IS&C)	US Coast Guard	US Coast Guard	16
3.71	MobiKEY Identity Based Access Device (MobiKEY IBAD) and Defense Identity Management Network (DEFIMNET)	Canada	Route1, Inc.	17
3.75	Mobile Tactical Edge Network (MTEN)	USNORTHCOM	Professional Software Engineering, Inc., pTerex, LLC	18
3.80	Riverbed Optimization System (RIOS)	US Air Force, DISA	C2I Solutions, Riverbed	18
4.79	Event-based Common Operational Picture (ECOP)	NGB	Booz Allen Hamilton	19
5.12	ID-MAP: Situational Awareness, Visualization and Collaboration (ID-MAP)	USNORTHCOM, US Coast Guard	General Dynamics	20
5.78	Next Generation - Joint Information Exchange Environment (NG-JIEE)	NGB	Koniag Services, Inc.	21
6.04	Tactical Emergency Asset Management (T.E.A.M.)	USNORTHCOM	Quantum Research International	21
6.53	Weapons of Mass Destruction Collaborative Analysis and Response System (WMD CARS)	USNORTHCOM	DTRA	24
6.66	Internet Protocol Interoperability and Collaboration System (IPICS)	Canada	Cisco Systems, Inc.	24
6.74	Security Information Management for Enclave Networks (SIMEN)	US Air Force	The MITRE Corporation	25
6.89	enhanced Video Text and Audio Processing (eViTAP)	US Joint Staff	Virage, Inc.	25
6.90	Optimized Data Environment for NetCentric Operations (ODEN)	DISA	TIMMES, Inc	26



U.S. MARINE CORPS SITE, DAHLGREN, VA.

Naval Surface Warfare Center

The U.S. Marine Corps, U.S. Army, U.S. Coast Guard and National Guard have selected NSWC Dahlgren Division, Dahlgren, Va., as their primary CWID 2007 site, including coalition forces land component commander (CFLCC) operations.

The Naval Surface Warfare Center Dahlgren Division (NSWCDD), a key contributor to the NAVSEA Warfare Center's team, consists of three sites: Dahlgren Laboratory, the Combat Direction Systems Activity Dam Neck, Va., and Coastal Systems Station Panama City, Fla. This year Dahlgren has the privilege to host the Coalition Force Land Component Commander (CFLCC), and three additional simulated afloat and ashore Command Centers. In addition, Dahlgren will participate in the Homeland Defense and Homeland Security initiatives led by the National Guard Bureau with support from the U.S. Coast Guard, U.S. Navy and U.S. Marines.

Under leadership of Captain Joseph McGettigan, USN, Commander NSWCDD, the warfare center's primary mission is to deliver solutions to the warfighter while continuing to build the Navy of the future in the most effective and efficient manner. The Dahlgren Division views the CWID as a unique opportunity to understand coalition warfighter capability gaps and to evaluate emerging technologies that can fill those gaps. Through continued development of acquisition workforce professionals, and with the strong commitment of CWID sponsors, NSWCDD sustains authority in the engineering and integration of complex systems. That authority has led to, and will continue to lead to, successful demonstration, thorough evaluation and accelerated delivery of effective, affordable and reliable solutions that meet warfighter needs. As future challenges arise NSWCDD plans to strengthen key partnerships and make critical investments that increase security and improve interoperability of coalition forces.

The Naval Sea (NAVSEA) Systems Command's on-going realignment of its warfare centers (both surface and underwater) continues in 2007 with the goal to build technical capacity across warfare centers, that can be harnessed without redundancy by Product Area Directors as identified by NAVSEA, to deliver products that meet Navy requirements of Sea Power 21. To that end, the Underwater and Surface Warfare centers were aligned into twelve Product Areas (PAs). Dahlgren Division is directly involved in building technical capacity across all three sites with six of those Product Areas: Surface Ship Combat Systems; Navy Strategic Weapon Systems; Ordnance; Littoral Warfare Systems; Homeland Force Protection; and Force Level Warfare Systems. NSWCDD is uniquely positioned to help navigate the road

NAVSEA WARFARE CENTERS

NSWC DAHLGREN DIVISION WEB SITE
http://www.nswc.navy.mil

SITE MANAGER
Bill Ormsby
540.653.8209
FAX: 540.653.0040
william.f.ormsby@navy.mil

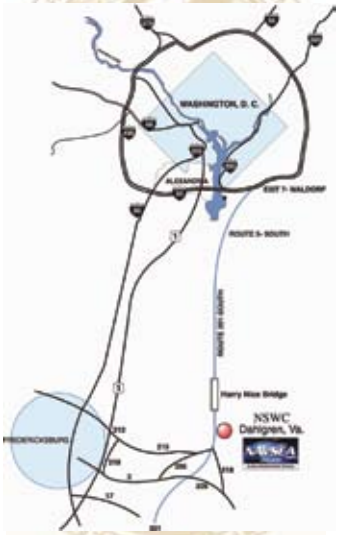
PROTOCOL CONTACT
Kathleen Rector
540.284.0870
FAX: 540.653.4679
kathleen.rector@navy.mil

MEDIA CONTACT
John Joyce
540.653.0365
FAX: 540.653.4679
john.j.joyce2.ctr@navy.mil

ALTERNATIVE PROTOCOL/ MEDIA CONTACT
Stacia Courtney
540.653.8154
stacia.courtney@navy.mil

to transformation. Its broad spectrum of resources, including workforce, infrastructure, and relationships with industry, have already made it a premier naval scientific and engineering institution that is dedicated to solving a diverse set of complex technical problems confronting the warfighter, whether on land, in the air, on the sea, or in space. Across its three sites, Dahlgren Division spent years building, testing, and stretching a technical infrastructure that is simply not available elsewhere.

The Division exists to understand technical dimensions of military problems, to know who can provide technical solutions to these problems and to know whether a responsible solution has been provided. This is accomplished by addressing three attributes of navy ownership: unimpeded access to intellectual facilities and resources, connectivity between the warfighter and the technical community, and a continuous source of competence to ensure integrity over the entire life cycle of a system. It can not be done alone; it requires sustained relationships with the warfighter, sponsors, industry and academia.



SECURITY
Val (Lucas) Shepherd
Valencia.Lucas@navy.mil
FAX: 540.653.6957

Voice confirmation:
540.653.5479

All security clearance information should be faxed to the security fax number.

FOREIGN REQUESTS
Brenda Bennett
540.653.3682
FAX: 540.653.4372
brenda.bennett@navy.mil

Barnita Byrd
540.653.8721
bamita.byrd@navy.mil

CWID Trials at NSWC Dahlgren Division

TRIAL NO.	SYSTEM TITLE (ACRONYM OR SHORT NAME)	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	TRIAL SECTION PAGE NO.
1.01	Compartmented High Assurance Information Network (CHAIN)	USEUCOM	Raytheon	3
1.17	Cross Domain Collaborative Information Environment/Collaboration Gateway (CDCIE/CG)	US Air Force, USJFCOM, FBI	Trident Systems	4
1.28	NET/X eToken Security System, Deployable Communication System (NET/X)	USJFCOM	FED-COMM USA, Inc.	4
1.54	Collaborate-Access-Browse (CAB)	NSA	Essex Corporation	5
1.55	Assured File Transfer (AFT)	NSA	CTC, Essex Corp., Tresys Technology	6
1.56	Owl Dual Diode (One-Way) Data Transfer System (Dual Diode)	Canada	Owl Computing Technologies, Inc.	6
1.63	Coalition Assured Sharing Environment (CASE)	DISA	General Dynamics	7
1.86	Federated Identity Management System (FIDMS)	USJFCOM	BearingPoint, Hewlett Packard	8
1.87	Federated Security (FS)	USJFCOM	SAIC, IBM, Sun	8
2.21	Commercial Joint Mapping Toolkit (CJMTK)	NGA	Northrop Grumman Corp.	10
2.57	Automated Image Mosaic and Mapping System (AIMM)	Canada	PCI Geomatics	11
2.88	AdLib	USNORTHCOM	EchoStorm, Inc.	11
3.09	Global Personnel Recovery System (GPRS)	US Air Force	Innovative Solutions International	12
3.14	Coalition Secure Management and Operations System (COSMOS)	DISA	Booz Allen Hamilton	12
3.27	Integrated Information Management System (IIMS)	US Army, US Air Force	US Army, US Air Force	13
3.31	Coalition Infrared Data Processing (CIDP)	US Air Force	Space and Missile Center, Missile Defense Agency	14
3.38	Collaborative Decision Aid (CDA)	USNORTHCOM	ARINC Engineering Services, LLC	15
3.39	Command, Control, Communications, Computers and Intelligence Defense (C4I Defense)	Italy	SELEX-Si SpA	15
3.48	Air Support Operations Center with Close Air Support System (ASOC Gateway with CASS)	US Air Force	US Air Force, US Navy	16
3.58	US Coast Guard Information Sharing and Communications (USCG IS&C)	US Coast Guard	US Coast Guard	16
3.70	Coalition open Joint Operations Picture (CoJOP)	UK	Fujitsu Services	17
3.71	MobiKEY Identity Based Access Drive (MobiKEY IBAD) and Defense Identity Management Network (DEFIMNET)	Canada	Route1 Inc.	17
3.75	Mobile Tactical Edge Network (MTEN)	USNORTHCOM	Professional Software Engineering, Inc., pTerex LLC	18
3.80	Riverbed Information Optimization System (RIOS)	US Air Force, DISA	C2I Solutions, Riverbed	18
4.79	Event-based Common Operational Picture (ECOP)	NGB	Booz Allen Hamilton	19
5.08	Joint Strike Fighter Off-board Mission Suppport Environment (JSF OMSE)	JSF Program Office	Lockheed Martin, Systematic Software Engineering, Naval Mission Planning	19
5.12	ID-MAP: Situational Awareness, Visualization and Collaboration (ID-MAP)	USNORTHCOM US Coast Guard	General Dynamics	20
5.78	Next Generation - Joint Information Exchange Environment (NG - JIEE)	NGB	Koniag Services, Inc.	21
6.13	Global Information Grid Quality of Service Edge Solution for Interoperability (GIG QoS ESI)	US Army	DSCI	22
6.66	Internet Protocol Interoperability and Collaboration System (IPICS)	Canada	Cisco Systems, Inc.	24
6.74	Security Information Management for Enclave Networks (SIMEN)	US Air Force	The MITRE Corporation	25
6.89	enhanced Video Text and Audio Processing (eViTAP)	US Joint Staff	Virage, Inc.	25
6.90	Optimized Data Environment for NetCentric Operations (ODEN)	DISA	TIMMES, Inc.	26



U.S. ARMY AT DAHLGREN

Gauging Operational Impact

The Army is collocated with the U.S. Marine Corps at Dahlgren. The Army's primary role in CWID is to participate in the investigation and evaluation of the CWID Interoperability Trials (ITs) and supported demonstrations.

The Army challenges the CWID ITs and local demonstrations to achieve significant improvements in the area of joint, coalition and interagency command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR). Evaluation of the CWID ITs and the Army's demonstrations assists the various Army Acquisition Commands in determining the operational effectiveness of CWID technologies. The Army will assist in evaluating C4ISR Interoperability Trials by manning a Tactical Operations Center and the ground portion of the Homeland Defense/ Security Operations Center.

GOALS FOR 2007

- Provide relevant and joint ready land power for the 21st century security environment
- Train and equip Soldiers to serve as warriors and growing adaptive leaders
- Sustain an All-Volunteer force composed of highly competent Soldiers
- Provide infrastructure and support to enable the force to fulfill its strategic roles and missions
- Improve the technology necessary to provide the leadership, decision making, and integration of Army Forces with other jointforces, multination-al forces, coalition forces, and interagency elements to conduct dominant maneuver, necessary situational awareness and intelligence, focused lo-gistics, precision fires, and full dimensional protection
- Link CWID to the Army's overall experimentation efforts, inserting information technology from the foxhole to the industrial base

CONTACT

John Saputo
HQDA G6
703 602 7364
john.saputo@hqda.army.mil



U.S. MARINE CORPS AT DAHLGREN

Flexible Operational Support

The United States Marine Corps is looking forward to participation in and evaluation of interoperability trials and Marine Corps demonstrations that will support warfighters and first responders in CWID 2007

The U.S. Marine Corps recognizes the importance of evaluating CWID interoperability trials (ITs) and Marine Corps-sponsored demonstrations. This venue allows Marine warfighters an opportunity to offer enhancements to interoperability solutions with coalition and joint forces, United States Federal agencies and bureaus.

The Marine Corps is extremely qualified to participate and evaluate ITs and demonstrations because the Corps is flexible in conduct of coalition and joint warfare, as well as supporting the Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), and U.S. Northern Command's (USNORTHCOM) Home Land Defense and Home Land Security (HS/HD) mission.

The Marine Corps continued to demonstrate flexibility this past year through support to coalition forces in Iraq and Afghanistan, enhancing coalition, joint and allied operations. The Marine Corps also provided first responders to support homeland contingencies and humanitarian relief in the United States and throughout the world.

CWID will continue to allow the Marine Corps to assess emerging interoperable technologies and demonstrations in coalition, joint and HS/HD operational arenas through cooperation with allied partners and government agencies.

The Marine Corps expects nothing less than outstanding results from assessment of trials and sponsored demonstrations that will support Marine Corps operating forces, whether working on the battlefield against terrorists or as first responders in disaster relief operations, while working with the various Coalition and Joint Forces, Federal Agencies and Bureaus. This worldwide demonstration will provide dynamic new technologies, which will strengthen the warfighter's and first responders' abilities and satisfy the Joint Staff, combatant commands, Services, agencies and bureaus goals.

MARINE CORPS C4ISR GOALS

■ **Build the Network**, which includes to develop future USMC IT in-fra-structure, develop the Marine Corps Enterprise Network, expand the USMC Expeditionary C4 capabilities, acquire integrated sys-tems, provide C4 guidance for C2 platform development, implement a USMC IT capital planning process, develop IT policies and stan-dards, and to establish governance over the network.

■ **Man the Network**, which includes to enhance the health of the C4 occupational field, and to ensure the C4 training and education satisfies the Marine Corps mission requirements.

■ **Populate the Network**, which includes to evaluate existing technologies (such as portals, collaboration tools, document and task management systems, and other web-based technologies), evaluate and identify new technologies to assist in problem solving, improve effectiveness, and promote efficiency, conduct business and technical analyses on proposed enterprises solutions to ensure that the network will be populated with those tools, applications, and systems that offer the greatest benefits to the Marine Corps, deploy IT solutions that provide analytical tools that leverage authoritative data sources fed by the data owners, and instantiate the USMC software baseline and application rationalization processes to ensure Marine Corps applications are interoperable with the network-centric views of Transformational Communications, GIG-BE, and USMC enter-prise.

■ **Protect the Network**, which includes to provide computer network defense, and to provide computer emergency response.

■ **Exploit the Network**, which will allow the Marine Air Ground Task Forces, joint, naval, and multinational (coalition) network operations, provide strategic agility (allowing rapid transition from a precrisis state to a full operational capability in a distant theater), provide operational reach to allow the projection and sustainment of relevant and effective power across the depth of the battle space, provide tactical flexibility by supporting multiple, concurrent, and dissimilar missions, and employ an agile supporting establishment.




U.S. NAVY SITE, SAN DIEGO, CALIF.

Space and Naval Warfare Systems Command

Rear Adm. Michael C. Bachmann, Commander, Space and Naval Warfare Systems Command (SPAWAR), hosts the U.S. Navy's site. SPAWAR's Office of the Chief Engineer designs the architecture and standards for FORCEnet, the Navy's vision for network-centric warfare and a key element of the Sea Power 21 philosophy.

Headquartered in San Diego, Calif., SPAWAR is a Navy acquisition command whose mission is to implement FORCEnet and transform information into decisive effects for naval and joint warfighters.

Team SPAWAR, consisting of diverse Program Executive Offices (PEOs), directorates and field activities, is uniquely composed to deliver network-centric capabilities to the Navy, the Department of Defense (DOD) and other government agencies.

OGAs

http://enterprise.spawar.navy.mil

SPAWAR is the only U.S. Navy CWID site that is co-located with an acquisition command. CWID's global demonstration provides acquisition authorities with valuable insight and opportunities to witness emerging C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) capabilities. Successful CWID solutions are recommended for inclusion in follow-on operational trials such as the Navy's annual Trident

Warrior series to achieve rapid operational deployment and program of record status.

ABOUT TEAM SPAWAR

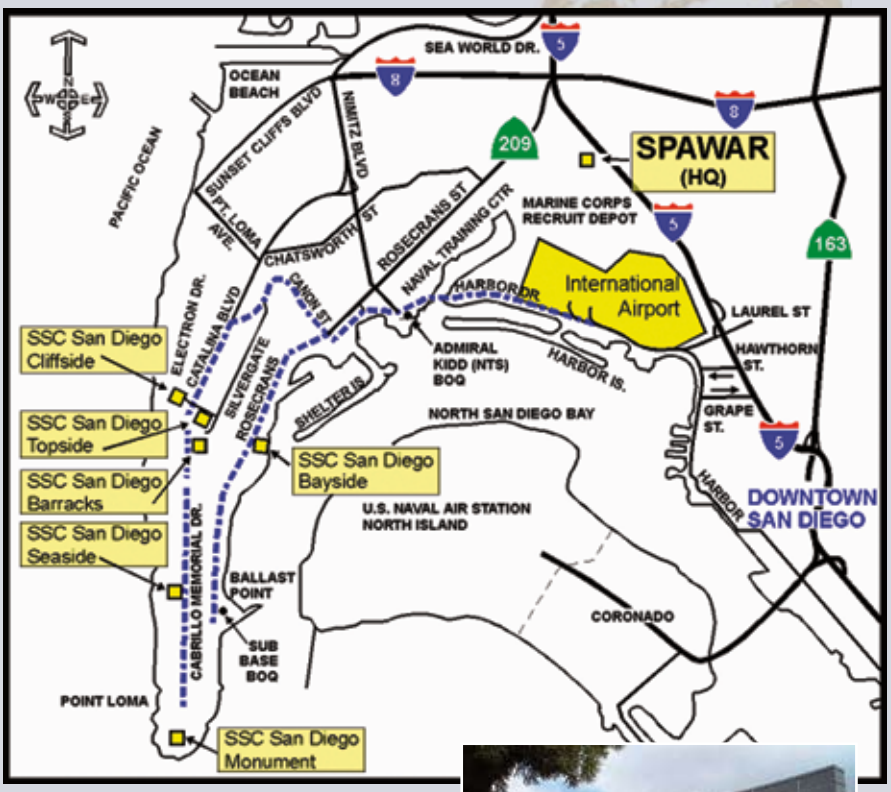
FORCEnet integrates warriors, sensors, command and control, platforms and weapons into a networked combat force, providing commanders the means to execute better, timelier decisions. But FORCEnet is more than a warfighting system; it also encompasses business strategies through the acquisition of C4I, business information technology and space systems. Ultimately, FORCEnet will significantly enhance knowledge superiority by allowing Navy and Marine Corps elements to link with joint, allied and coalition forces through seamless interoperability within DOD's Global Information Grid.

SPAWAR's Office of the Chief Engineer develops the FORCEnet architecture and standards while associated PEOs apply the architectures and standards to acquire, align and field more than 150 C4I systems to help make the FORCEnet vision a reality.

Our PEO partners include: PEO C4I, San Diego, Calif.; PEO Space Systems, Chantilly, Va.; and PEO Enterprise Information Systems, Arlington, Va.

In addition, SPAWAR supports the Joint Program Executive Office for the Joint Tactical Radio System San Diego, an essential program that will modernize interoperable DOD communications.

SPAWAR's Systems Centers are located in New Orleans, La., San Diego, Calif., Charleston, S.C., and Norfolk, Va. The SPAWAR Space Field Activity is in Chantilly, Va., and the Washington Liaison Office is in the nation's capital.



SPAWAR Headquarters is located in San Diego's Old Town just west of Interstate 5 at 4297 Pacific Highway. Exit "Old Town" from 5 South, or exit "Pacific Highway" from 5 North.

VISITOR'S RECEPTION is located just north of the pedestrian bridge. The CWID site is located in Building OT-3, 2nd Floor, East Mezzanine, Rooms 2430, 2434, 2438.

INTERNATIONAL VISITOR FOREIGN VISITS OFFICE

Adam Valecruz
adam.valecruz.ctr@navy.mil
foreign@spawar.navy.mil
619-524-7289 Voice
858.537.0127 Fax

POC FOR VISIT

Robert Whitney SSC-SD
Code 2644
858.537.0206
858.537.0153 Fax

VISIT REQUEST ADDRESS

SPAWARSYSCEN
SAN DIEGO
Attn: Visitor Control OTC
53560 Hull Street
San Diego CA 92152-5001

619.524.2745 Fax
619.524.2751 or 3124

(for verification)

PERSONS TO BE VISITED

Robert Whitney
SSC-SD Code 2644
858.537.0206

Ron Anderson
SSC-SD Code 2644
858.537.0204

ENTERPRISE APPROACH: THE NAVAL NETWAR FORCENET ENTERPRISE

The Navy's acquisition organizations that support the Air, Surface, Submarine, Expeditionary and Network communities have realigned under an enterprise model to increase efficiency, decrease costs and improve speed to capability for the Fleet.

The Naval NETWAR FORCEnet Enterprise, or NNFE, is an enterprise approach to implementing FORCEnet and delivering network-centric capabilities. This is a collaborative effort between the Naval Network Warfare Command (NETWARCOM), Office of the Chief of Naval Operations N6 (OPNAV N6), SPAWAR and additional stakeholder organizations.

The NNFE's Board of Directors is led by top admirals who assess the enterprise's progress in delivering its products and services. The NETWARCOM Commander is the Chief Executive Officer, OPNAV N6 is the Chief Financial Officer and the SPAWAR Commander is the Chief Operating Officer.

The NNFE develops processes and metrics across the enterprise to help the Navy better understand the costs of conducting business and how it relates to readiness. It will allow the enterprise to make better decisions when applying critical resources – both dollars and manpower – and provide the right products and services to the warfighter faster and more efficiently.

VISITOR REQUESTS, ACCESS AND PARKING

www.spawar.navy.mil/sandiego/
- Select "San Diego" under Systems Center
- Select "About SSC San Diego"
- Navigate to "Visitor Information"

■ **CWID'S U.S. NAVY SITE** is located at SPAWAR in San Diego, Calif. The SPAWAR CWID Team assembles a joint, coalition, and civilian authority staff; matching trial requirements to support from Navy, Marine, Coast Guard, and local civilian agencies.

For the CWID 2007 execution scenario, SPAWAR is also home to the Combined Forces Maritime Component Commander (CFMCC) and USNORTHCOM's west coast homeland security site.

CWID Trials at SPAWAR

TRIAL NO.	SYSTEM TITLE (ACRONYM OR SHORT NAME)	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	TRIAL SECTION PAGE NO.
1.01	Compartmented High Assurance Information Network (CHAIN)	USNORTHCOM	Raytheon	3
1.05	Trusted Gateway System Guard (TGS-Guard)	US Air Force	US Air Force	3
1.28	NET/X eToken Security System, Deployable Communications System (NET/X)	USJFCOM	FED-COMM-USA, Inc.	4
1.43	Mobile Forces Solution - Subnet Relay (MOFS-SNR)	Germany	T-Systems Enterprise Services GmbH	5
1.54	Collaborate-Access-Browse (CAB)	NSA	Essex Corporation	5
1.55	Assured File Transfer (AFT)	NSA	CTC, Essex Corp., Tresys Technology	6
1.56	Dual Diode (One-Way) Data Transfer (Dual Diode)	Canada	Owl Computing Technologies, Inc.	6
2.06	Italian Navy Maritime Command and Control Information System (MCCIS-Italy)	Italy	MARITEL-Roma	9
2.21	Commercial Joint Mapping Toolkit (CJMTK)	NGA	Northrop Grumman Corp.	10
2.57	Automatic Ingest, Mosaic and Mapping System (AIMM)	Canada	PCI Geomatics	11
3.22	Scalable Mesh Networks	US Navy	OrderOne Networks	13
3.70	Coalition Open Joint Operations Picture (CoJOP)	UK	Fujitsu Services	17
3.71	MobiKEY Identity Based Access Device (MobiKEY IBAD) and Defense Identity Management Network (DEFIMNET)	Canada	Route1 Inc.	17
4.79	Event-based Common Operational Picture (ECOP)	National Guard Bureau	Booz Allen Hamilton	19
5.12	ID-MAP: Situational Awareness, Visualization and Collaboration (ID-Map)	USNORTHCOM US Coast Guard	General Dynamics	20
5.78	Next Generation - Joint Information Exchange Environment (NG-JIEE)	National Guard Bureau	Koniag Services, Inc.	21
6.04	Tactical Emergency Asset Management (T.E.A.M.)	USNORTHCOM	Quantum Research International	21
6.13	Global Information Grid Quality of Service Edge Solution for Interoperability (GIG QOS ESI)	US Army	DSCI	22
6.42	HotZone 4010/4020 (HZ 4010/4020)	US Navy	Trimax Wireless, Inc.	23
6.53	Weapons of Mass Destruction Collaborative Advisory Response System (WMD CARS)	USNORTHCOM	DTRA	24
6.89	enhanced Video Text and Audio Processing (eViTAP)	US Joint Staff	Virage, Inc.	25
6.90	Optimized Data Environment for NetCentric Operations (ODEN)	DISA	TIMMES, Inc.	26



U.S. AIR FORCE SITE, HANSCOM AIR FORCE BASE, MASS.

Electronic Systems Center

NATIONAL MILITARY STRATEGY

"...creation of a collaborative information environment that facilitates information sharing, effective synergistic planning, and execution of simultaneous, overlapping operations... on demand to defense policymakers, warfighters and support personnel."

2007, CHAIRMAN, JOINT CHIEFS OF STAFF

Electronic Systems Center (ESC)(Air Force Materiel Command) is Hanscom's host organization. Activated April 1, 1961, ESC manages development and acquisition of electronic command and control (C2) systems that collect and analyze information on potentially hostile forces, enabling commanders to make quick, accurate decisions and rapidly direct forces, America's airpower, to the right target at the right time.

ESC is the Air Force's leader in C2 programs. It manages nearly 200 programs and an annual budget of approximately $3 billion.

In 2001 the Air Force gave ESC the lead to integrate its C2, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems--the C2 Enterprise. Integrated C4ISR capabilities provide an asymmetric force advantage and enable development of network-centric warfare. Today ESC integrates systems within the Enterprise to eliminate "stovepipes" and to ensure warfighters have the capabilities they need to achieve their objectives.

We are transforming the battlespace; creating a new paradigm where net-centricity is an essential information-centric warfighting capability.

SUPPORTING THE WARFIGHTER – DELIVERING CAPABILITIES

CONTACTS

CFACC
Lt Col Robert Pagoni
Global Cyberspace Integration Center (GCIC)
robert.pagoni@hanscom.af.mil

SITE MANAGER
Capt Jesse Jaramillo
644th ELSS/CEIF
Ext. 1160
jesse.jaramillo@hanscom.af.mil

SITE COORDINATOR AND PUBLIC AFFAIRS
Mr. Ronald Goodner
753rd ELSG/XR, Ext. 6397
ron.goodner.ctr@hanscom.af.mil

2007 PRIORITIES

The ESC Commander set priorities for 2007 that will drive the entire organization. Among them: continue to achieve acquisition excellence — delivering war-winning

capability to the warfighter is at the very core of what we do; we will keep our programs on time and on cost; deliver value to the warfighter — clear communication and regular interaction with our customers are absolutely essential to our success and their success on the battlefield.

2006 SUCCESS STORIES

In 2006, ESC's acquisition community scored many successes. Among them: an Improvised Explosive Device Defeat (IEDD), Ground Moving Target Indicator (GMTI) forensic analysis tool was fielded five months following receipt of the Mission Needs Statement; installed over 50 AN/FMQ-19 systems, an automated and integrated weather reporting system, providing safer and more efficient air operations worldwide, including Iraq and Afghanistan; delivered 10,000 Combat Survivor Evader Locator (CSEL) radios, officially credited with saving 30 lives in Afghanistan; GeoBase deployment on GCSS-AF accelerated delivery of imagery and maps to combatant commanders – reduced access times up to 90%; hits up 500%, data moved up 300%; upgraded security for 16 CENTAF bases in eight countries; upgraded AUAB CAOC in the heat of the battle, giving CFACC C2&ISR tools to identify and destroy terrorist targets; fielded AOC 10.1 to Ramstein AB, Hickam AFB, Korea, Al Udeid, FTU, and help desk, providing common world-wide AOC baseline; fielding teams praised by 3-star CFACC/JFACCs; Reduced Crypto Key Load Time for F-22 FIREFLY from 4 to 1.5 hours; successful Proteus test bed fielded Sept. 30, 2006 — provides next generation GMTI; improved GWOT C2 capability by increased communications planning support to CENTAF AOR locations.

ESC is organized for success! At Hanscom, four acquisition wings responsible for Enterprise Integration, Battle Management, C2ISR, Operations Support, respectively, and two geographically separated Groups, an Engineering Installation Group and a Cryptologic Systems Group, report to a single commander, the ESC Commander, dual-hatted as PEO for C2 and CS. Infrastructure support is provided by an Air Base Wing. This powerful organization is providing net-centric capabilities to our warfighters TODAY!

CONTACTS

Hanscom AFB dialing:
Comm'l: 781-377-XXXX
DSN: 478-XXXX

SITE NCOIC

MSgt Chris Anderson
644th ELSS/CEIF
Ext. 6548
chris.anderson@hanscom.af.mil

NETWORK ENGINEERING

Mr. Bill Page
644th ELSS/CEIF
Ext. 8458
william.page.ctr@hanscom.af.mil

SYSTEMS ENGINEERING

Mr. Matt Galster
644th ELSS/CEIF
Ext. 5390
matthew.galster.ctr@hanscom.af.mil

NET CENTRIC OPERATIONS: THE DRIVING OPERATIONAL CONCEPT

SCENARIO AND ARCHITECTURE

Mr. Bob Gee
644th ELSS/CEIF
Ext. 6666
robert.gee.ctr@hanscom.af.mil

NETWORK CERTIFICATION AND ACCREDITATION

Mr. Larry Barrows
644th ELSS/CEIF
802-859-0341
larry.barrows.ctr@hanscom.af.mil

COMSEC CUSTODIAN

Mr. John McElhinney
644th ELSS/CEIF
Ext. 5535
john.mcelhinney.ctr@hanscom.af.mil

SITE SECURITY AND

653RD ELECTRONIC SYSTEMS WING (653D ELSW)

One of four acquisition wings at ESC, the mission of the 653d ELSW is to identify technology opportunities to improve C4ISR, provide an integrated environment for examining innovative aerospace operational concepts and to ensure C4ISR products are fully compatible and interoperable.

753RD ELECTRONIC SYSTEMS GROUP

The 753d ELSG was created within the 653d ELSW to lead integration, development, certification, deployment and sustainment of Air Force, Joint, and Coalition C4ISR combat capabilities. The products are fully compatible and interoperable.

The 753rd is ideally positioned to support CWID and other C4ISR programs. The 753rd has a highly skilled work force conducting systems engineering and capability integration. The Group has at it's disposal powerful enablers such as Cursor on Target, Air Force Modeling and Simulation Training Toolkit, and Collaboration Development Environment.

THE GROUP ALSO HAS:

- Accessibility to other acquisition organizations
- The experience to conduct acquisition from the warfighter's perspective
- Its own risk reduction capabilities
- Spiral development experience
- Acquisition acceleration techniques
- On-going capability development and transition activities
- Long-term experience in JFEX

TECHNOLOGY TRANSITION

The 753d ELSG conducts technology planning and pre-Milestone A/B preparation activities to support technology transition. The Group is responsible for oversight and management of technology programs such as the Applied Technology Council (ATC), Small Business Innovation Research (SBIR), and

MITRE Mission Oriented Investigation and Experimentation (MOIE) programs) sponsored by ESC. The Group helps identify programs of record at ESC to which technologies are targeted for transition. In addition, programs are identified that may share similar needs and provide additional or alternate avenues for transition of high-payoff technologies.

NESI AND TIA OBJECTIVE

DISCIPLINED STANDARDS AND GOVERNANCE ACROSS THE ENTERPRISE – INTEGRATION THROUGH STANDARDS

THE VISION: AN INTEGRATED ENTERPRISE

The vision is to have a Global Information Grid (GIG), in which all C2 assets are connected. The GIG will contain an infrastructure that allows platforms to be connected and to seamlessly share information. The GIG encompasses the four combat domains: Space, Air, Terrestrial (Land and Sea), and now Cyberspace.

Regardless of what the conflict is or where it is, we need to be dynamic, flexible, and able to adapt to any situation and manage the information on the network. In the final analysis, the best information is available to the decision makers in a timely manner.

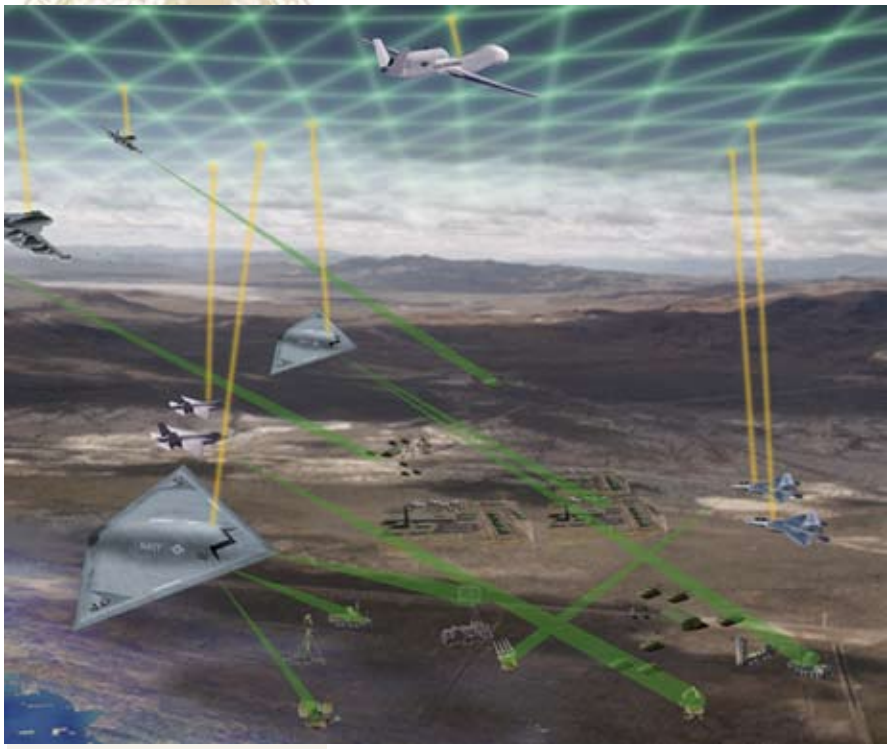
The GIG is a combination of assets that can communicate and share information to achieve the proper effects. The GIG requires an architecture that is flexible enough to allow continued communications and exchanges, regardless of the time, place, number of conflicts, military objectives, or situation.

ACHIEVING THE VISION THROUGH ACQUISITION INNOVATION

The acquisition community must implement a variety of new processes and procedures to achieve the transformation to net-centricity. One example is Net-Centric Enterprise Solutions for Interoperability (NESI).

NET-CENTRIC ENTERPRISE SOLUTIONS FOR INTEROPERABILITY (NESI)

NESI is a cross-service effort between the USAF (ESC - Program Executive Office (PEO) C2 & CS), the Navy (PEO for C4I and Space), DISA and the Army CIO. NESI provides implementation guidance to facilitate the design, development and use of information systems for net-centric warfare. This process is accomplished through a Strategic Technical Plan and a set of standards and implementations that allow programs to build their information in a way that conform to the standards.



VISIT REQUESTS

Mr. Vinnie Cook
644th ELSS/Security
Ext. 9775 or 9485
FAX Ext. 2200
vinnie.cook.ctr@hanscom.af.mil

FOREIGN VISITOR CONTACT

Mr. Clark Foreid
753rd ELSG/CO, Ext 4199
FAX: Ext. 2200
clark.foreid@hanscom.af.mil

VISIT REQUEST INFORMATION

FAX to Ext. 2200 or
to JPAS SMO Code LK1MFB956
753rd ELSG/Security
Purpose: CWID 07
Gov't POC: Capt Jesse Jaramillo
15 Eglin Street, Bldg 1607
Hanscon AFB, MA 01731
To confirm reciept:
Mr. Vinnie Cook (see above)

VISIT REQUEST AND SHIPPING ADDRESS

753rd ELSG/CO
Attn: Mr. Gil Ynostroza
CWID 07
15 Eglin Street, Bldg 1607
Hanscom AFB, MA 01731
Ext. 2152, Fax Ext. 2200
gil.ynostroza@hanscom.af.mil

GENERAL INFORMATION

about Hanscom AFB and ESC may be found at:
http://esc.hanscom.af.mil

The overall goal is to provide common, cross-service guidance in basic terms for program managers and developers of net-centric solutions. All users can tie into a common communication network. Depending on where they are in each of these nodes they'll have access to any information on the net that is built on open standards. All information available on the network must be accessible to everyone in an open standard that everyone understands.

OBJECTIVE

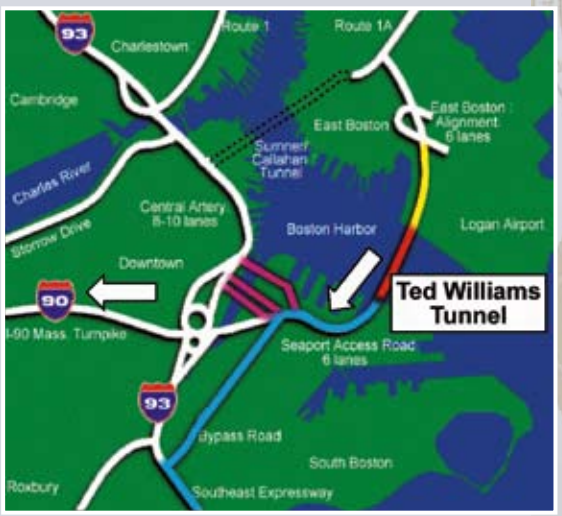
FIELD BETTER, CHEAPER NET-CENTRIC APPLICATIONS EARLIER

The framework allows programs to build their information so it can be discoverable and easily transmitted and received across the different nodes within the theater. This is enterprise integration. ESC is developing sound policies, guidance and direction to ensure the effective use of scarce resources to achieve the desired value and benefits inherent in enterprise integration.

TECHNICAL IMPLEMENTATION ARCHITECTURE (TIA)

The goal is to establish one TIA for Air Force C2 systems. Having one TIA will eliminate duplication of effort by specifying architecture and infrastructure. The Architecture will define consistent technical requirements and contractual language for C2 program compliance. It will also pre-qualify a "short list" of commercially integrated solutions, and engi-

Directions to Hanscom Air Force Base



LOGAN INTERNATIONAL AIRPORT/BOSTON

- Upon leaving Logan, follow signs to I-90 West/ Ted Williams Tunnel
- After the Tunnel, keep following I-90 West toward Exit 15
- Take Exit 15 to access I-95/Rt 128 North
- Continue on I-95 North to Exit 30
- Take Exit 30 and continue on to Exit 30B, Hanscom Field/Concord
- Take Rt 2A West (Marrett Rd) and follow signs to Hanscom Field/ AFB
- Register your vehicle at the Visitor Center (Vandenberg Gate)

VANDENBERG GATE

VISITOR CENTER HOURS 6:00 AM to 10:00 PM

neer enterprise-driven, specific solutions.

TIA will establish an overall governance framework to manage and enforce compliance with the TIA specifications, standards and contract language.

The 753rd's involvement in these activities and our access to highly qualified technical and acquisition personnel across ESC and the state-of-art C4ISR Enterprise Integration Facility (CEIF), allows us to provide to CWID and other customers, a plug-and-play environment for collaboration, evaluation, integration and assessment of emerging technologies.

Trials at Hanscom Air Force Base

TRIAL NO.	SYSTEM TITLE (ACRONYM OR SHORT NAME)	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	TRIAL SECTION PAGE NO.
1.01	Compartmented High Assurance Information Network (CHAIN)	USNORTHCOM	Raytheon	3
1.05	Trusted Gateway System (TGS) Guard	US Air Force	US Air Force	3
1.54	Collaborate-Access-Browse (CAB)	NSA	Essex Corporation	5
1.55	Assured File Transfer (AFT)	NSA	CTC, Essex Corp., Tresys Technology	6
1.86	Federated Identity Management System (FIDMS)	USJFCOM	BearingPoint, Hewlett Packard	8
2.37	Rapid Force Warning (RFW)	US Army	US Army	10
3.09	Global Personnel Recovery System (GPRS)	USJFCOM	Innovative Solutions International	12
3.30	Spatio-Temporal Analysis for Rapid Tasking (START)	US Air Force	The MITRE Corporation	14
3.31	Coalition Infrared Data Processing (CIDP)	US Air Force	Space and Missile Center, Missile Defense Agency	14
3.39	Command, Control, Communication, Computers and Intelligence Defense (C4I Defense)	Italy	SELEX-SI SpA	15
3.48	Air Support Operations Center with Close Air Support System (ASOC Gateway with CASS)	US Air Force	US Air Force, US Navy	16
3.70	Coalition open Joint Operations Picture (CoJOP)	UK	Fujitsu Services	17
3.71	MobiKEY Identity based Access Drive (MobiKEY IBAD) and Defense Identity Management Network (DEFIMNET)	Canada	Route1, Inc.	17
3.80	Riverbed Information Optimization System (RIOS)	US Air Force, DISA	C2I Solutions, Riverbed	18
4.79	Event-based Common Operational Picture (ECOP)	National Guard Bureau	Booz Allen Hamilton	19
5.08	Joint Strike Fighter Off-board Mission Support Environment (JSF OMSE)	JSF Program Office	Lockheed Martin, Systematic Software Engineering, Naval Mission Planning	19
5.59	Mission Planning System (MPS)	US Air Force	Collaboration Technolgies, Inc.	20
5.78	Next Generation-Joint Information Exchange Environment (NG-JIEE)	National Guard Bureau	Koniag Services, Inc.	21
6.53	Weapons of Mass Destruction Collaborative Advisory Response System (WMD CARS)	USNORTHCOM	DTRA	24
6.74	Security Information Management for Enclave Networks (SIMEN)	US Air Force	The MITRE Corporation	25

OBJECTIVE

FOCUS ON ADDING OPERATIONAL VALUE

COALITION AIR OPERATIONS CENTER (CAOC)

During CWID 2007, Hanscom AFB hosts the Coalition Force Air Component Commander (CFACC). Key Coalition Air Operations Center (CAOC) leadership positions are simulated to facilitate the CWID assessment process and are located in the C4ISR Enterprise Integration Facility (CEIF).

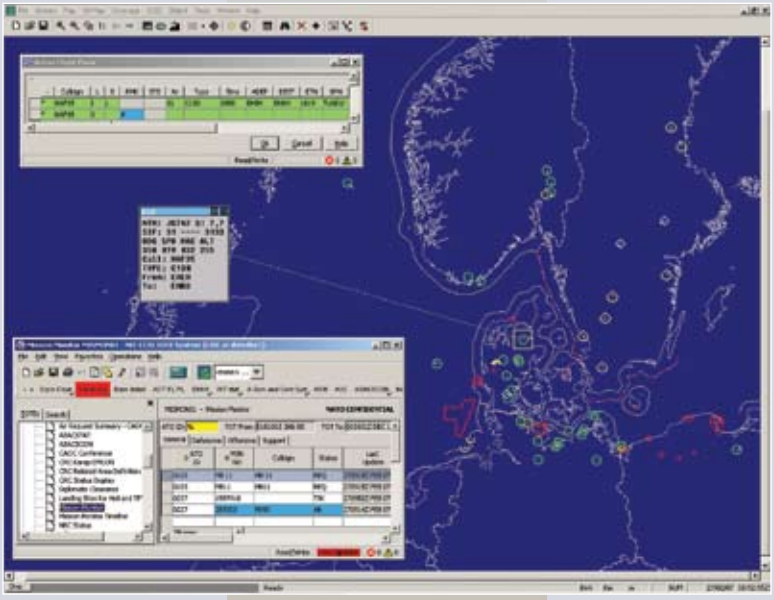
USAF personnel and Coalition partners are role players in the Combat Plans and Combat Operations cells of the CAOC. Planners prepare the Air Tasking Order (ATO) and Airspace Control Order (ACO).

Together with the Master Scenario Events List (MSEL), the ATO provides the backdrop to assess potential enhanced capability for the warfighter provided by the various Interoperability Trials (ITs).

ESC also hosts ITs in support of US-NORTHCOM to evaluate emerging technologies for local and Federal agencies involved in Homeland Defense and Homeland Security (HS/HD). Ultimately, ESC champions the concepts and capabilities of Net-Centricity for U.S., NATO, Coalition and HS/HD forces.

Air Operations Translated

NORTHERN EUROPEAN COMMAND – COMMAND AND CONTROL INFORMATION SYSTEM (NEC CCIS) is a flexible and versatile tri-service Command and Control (C2) system. NEC CCIS offers C2 functionality on all levels and operational areas with emphasis on air operations. The system is sponsored and operated by NATO, Denmark and Norway. Sites are fielded in Poland and soon in the Baltic States. NEC CCCIS has been deployed in live missions several times.



The system is one of two NATO C2 systems used for air operations in Europe. NEC CCIS supports full automatic data exchange from Air Component Commander to Coalition Air Operations Center (CAOC), Wing and Squadron level in Denmark and Norway. Data handling, Mission Monitoring and reporting is feasible on all levels. Mission planning data can be exported to Portable Flight Planning System (aircraft planning system).

NEC CCIS interoperability was demonstrated during CWID 2006 in order to enhance interoperability with U.S. Air Force Theater Battle Management Core Systems (TBMCS). The system can receive data in United States Message Text Format (USMTF) and Over-the-Horizon (OTH) OTH-Gold format. NEC CCIS can translate the imported messages, such as Air Tasking Orders (ATOs) and Airspace Coordination Orders (ACOs), from USMTF format to NATO ADatP-3 format.

NEC CCIS is currently based on a Solaris Server with Windows 2000 clients using the eXtensible Markup Language (XML) and java for operational functionality. The NEC CCIS system provides a configurable user interface with XML capabilities, allowing the system to easily adapt to operational requirements.

NEC CCIS, version R12, has a formal NATO security accreditation for NATO SECRET in the System High mode of Operation.

SYSTEM CONTACTS

DENMARK

Tactical Air Command Denmark
Capt. Christian Willer
+ 45 2268 1591
Willer@mil.dk

HANSCOM

Capt. Jesse Jaramillo
781-377-1160
jesse.jaramillo@hanscom.af.mil

Mr. Robert Gee
781-377-6666
robert.gee.ctr@hanscom.af.mi



PENTAGON: WARFIGHTER CAPABILITY DEMONSTRATION CENTER

Informing Senior Leadership

The Warfighter Capability Demonstration Center (WarCap, previously C4ISR Visualization Center, or CVC), creates a live, immersive portal to provide decision makers insight into the value and achievements of CWID.

Located in the Pentagon, the WarCap differs from other CWID locations in that live trials will be presented via advanced distributed technologies. Presentations at the facility will complement site visits by highlighting a representative cross section of CWID interoperability trials and participants from other U.S. sites and U.S. European Command (USEUCOM).

Using a variety of robust visualization and conferencing tools on the exercise network, the WarCap will feature selected trials from multiple sites, placing attendees at the center of the event, during each hour-long presentation.

Pentagon attendees will be able to interact with subject matter experts from each location in real time, a valuable opportunity for those unable to travel to all the sites they would like to visit.

CONTACT

Anna L. Santos de Dios
Exercise Planning Lead
703-693-0410 (DSN 223)

DAILY SCHEDULE

JUNE 19 to 21
9 A.M. USEUCOM, NSWC Dahlgren, Hanscom AFB
11 A.M. USNORTHCOM, SPAWAR, Hanscom AFB
(11 a.m. session June 21, reserved for media only)

INDIRECT FIRE FORWARD AIR CONTROL TRAINER DEMONSTRATION FOR SENIOR AIR FORCE LEADERS IN THE WARCAP

WARFIGHTER CAPABILITY DEMONSTRATION CENTER GOALS

INCREASE CWID VISIBILITY

■ Ideally situated in the National Capitol Region, the WarCap aims to broaden CWID's exposure to senior military leaders to members of Congress and their staffs, representatives of government agencies beyond DoD, and members of the media.

LAY THE FOUNDATION

■ 2007 represents the WarCap's first year of support to CWID. The connectivity and relations established during this round of presentations will enable greater support to CWID in future years.



NATIONAL GUARD DEMONSTRATION SITES

States Key Scenario Responders

The Delaware, Colorado, California, Massachusetts, and New York National Guard support roleplayers and operators required to execute scenario events. In addition, the National Guard supports two state demonstration sites, Mountaineer CWID, W.Va., and Palmetto CWID, S.C.

MOUNTAINEER CWID

The West Virginia Department of Military Affairs and Public Safety (WVDMAPS), as the cabinet level executive agency for state emergency management, in conjunction with the West Virginia National Guard (WVNG), will host two interoperability trials as part of the "Mountaineer" CWID site.

The WVDMAPS will leverage participation in CWID 2007, as well as the selected interoperability trial technologies, to conduct a Joint-Interagency Emergency Management Exercise at multiple locations throughout West Virginia based on a spontaneous "Urban to Rural" (U2R) mass evacuation of the National Capital Region (NCR) in response to a simulated terrorist attack in the nation's capital. The exercise will focus on state, county and local emergency management agencies' plans for responding to an "Urban to Rural" migration of evacuees and the mitigation of those effects on the local infrastructure in the State of West Virginia.

The sponsored interoperability trials, IT 3.75 pTerex Mobile Tactical Edge Network (MTEN), and IT 6.04 First Response Tactical Emergency Asset Management (T.E.A.M.), were selected for demonstration in support of WVDMAPS and WVNG objectives for Cross-Domain Data Sharing, Integrated Operations, Planning and Communications. The pTerex MTEN will be deployed as an asset to WVNG Liaison Officer (LNOs) assisting local emergency mangers in a Defense Support to Civil Authorities mission. The First Response T.E.A.M. will be deployed as an asset to the WVDMAPS and local emergency managers to enhance interoperable communications to a civil emergency response.

These interoperability trials will be integrated into existing state and local communication systems, as well as the WVNG's Joint Incident Site Communications Capabilities (JISCC) and Interim SATCOM Incident Site Communications Set (ISISCS) mobile communication packages. Civil Air Patrol (CAP) wings from West Virginia, Virginia, Maryland and Pennsylvania will additionally provide near real time aerial imagery of evacuation routes to emergency operations centers throughout the state for situational awareness and incident mitigation. Multiple CAP aircraft from the participating wings will provide this information through the Satellite-transmitted Digital Imaging System (SDIS) and Airborne Real-time Cueing Hyperspectral Enhanced Reconnaissance (ARCHER) systems. Such vital information will be relayed through the selected interoperability trials, IT 3.75 and IT 6.04, and shared through the CWID portal to "paint the common operational picture" at multiple levels of government agencies and military commands.

The WVNG will provide information and data input to the National Guard Bureau's

CONTACT
MAJ Kory Gacono
C4 Integration / Joint Information Exchange Environment (JIEE) Program Manager
kory.gacono@us.army.mil

(NGB) sponsored interoperability trials IT 4.79 National Guard - Event-based Common Operational Picture (NG-ECOP) and IT 5.78 Next Generation - Joint Information Exchange Environment (NG-JIEE). The WVNG will leverage participation with the NG-ECOP to populate the COP with actual deployed and "notionally" engaged units and assets. NG-JIEE will be utilized for event information management, to process Requests for Information (RFIs) and Requests for Assistance (RFAs), and to support critical event information sharing, reporting and situational awareness.

The participation of the WVDMAPS, the WVNG, and local emergency management agencies in CWID 2007 will enhance interoperable communications and data sharing, improve our abilities to conduct integrated operations, planning and communications, and further ensure that we are prepared to meet the needs of our state's and nation's citizens in times of crisis.

PALMETTO CWID

Over 500 soldiers and airmen of the South Carolina National Guard began the 2006 Hurricane Season in June in North Charleston, South Carolina, by participating in a two-week, emergency communications demonstration called Palmetto Coalition Warrior Interoperability Demonstration, or Palmetto CWID.

The purpose of Palmetto CWID in 2006 was to validate the "first responder" emergency communications plans of the Department of Homeland Security and U.S. Northern Command, as well as test incident area communications interoperability. Since the devastating hurricane season of 2005, the military, state and federal agencies, and industry have been working closely to develop, and test state-of-the-art communications assets that can interoperate with local police, fire, and rescue radios in the aftermath of a catastrophic event.

the National Guard will leverage CWID scenarios and simulated operational networks to test improved operations and coordinate Homeland Defense and Defense Support to Civil Authorities (HD/DSCA) response.

At the end of each hurricane season, Maj. Gen. Stan Spears, the Adjutant General of South Carolina asks the S.C. National Guard leadership, 'what can we do to help ensure we are better prepared to help our neighbors next year?' Palmetto-CWID helps answer that question by providing a venue in which all levels of government, the military and industry are working together to better prepare for future disasters.

CWID provides a venue ot test operations and interoperability of the Joint Incident Site Communications Capability (JISCC), a capability developed and fielded to the States and Territories by the National Guard Bureau to meet communications, reachback, and interoperability requirements at the incident area. CWID will enable testing of related communications capabilities, such as IT 3.75 pTerex Mobile Tactical Edge Network (MTEN). In addition, Palmetto CWID participants will be able to communicate RFIs and RFAs and situation reporting to the state and national levels using the Natonal Guard Joint Information Exchange Environment interoperability trial. The movement and position of the JISCC will be tracked using through the National Guards other CWID trial - E-COP - which will support the NGB Joint C4 Coordination Center in it's tracking of C4 assets.

NATIONAL SECURITY AGENCY, FORT MEADE, MD.

Finding Vulnerable Back Doors

November 7, 2001, the Senior Management Group of the Joint Warrior Interoperability Demonstration (JWID, now CWID) program commissioned NSA to perform a security assessment of interoperability trials that participate in the event.

NSA's approach is consistent with the National Security for Telecommunications and Information Systems Security Policy "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products" and the National Information Assurance Program (NIAP). Security assessment results may be input to security design (e.g. NIAP validation) and the Certification and Accreditation (C&A) processes (e.g. DITSCAP, NIACAP).

SECURITY ASSESSMENT APPROACH

NSA models the "security environment" in terms of "threats" (or threat events) anticipated for an operational deployment, policy statements that apply, and assumptions about how trial capabilities will be used. Respective trials are assessed against this model of the security environment to determine how the capability counters each identified threat, and enforces each identified policy, consistent with assumptions regarding how the capability will be used. Mapping between the warfighter's security environment and the trial's specific security countermeasures, NSA performs a security protection coverage and exposure analysis. Coverage analysis identifies threats specifically addressed by the demoonstration or trial. Exposure analysis identifies threats handled by the environment where the capability is deployed, representing actual "security benefits."

RESULTS OF SECURITY ASSESSMENT

2007 is the sixth year NSA has performed Security Assessments with CWID (formerly known as JWID). NSA continues to collect data on the effectiveness of the assessment. "Gold Nuggets" from JWID 2001-2002 did commit to having security protection implemented within their products validated through the NIAP process. One vendor was successful taking two products through the NIAP process: BMC Software PATROL® was certified by NIAP September 30, 2002; and PATROL® Perform/Predict was certified April 8, 2002. Other JWID/CWID vendors reported enhancements to the security of their products, but have not yet validated them with a NIAP Accredited Laboratory.

NSA performed Security Assessments for 2006. Criteria determining which trials will be assessed in CWID is based on the NSTISSP No.11, which targets IA and IA-enabled products. The Security Assessment report that is generated through the CWID Security Assessment Process can be used directly by vendors to create Security Target documentation, or by security practitioners to create a Protection Profile for their respective IA needs. The report also identifies specific security coverage areas and protection exposures that should be addressed as part of a formal C&A of every operational deployment of these capabilities.

ADDRESS

NSA
9800 Savage Rd.
Ft. Meade, MD 20755

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

Supplying the Space-Eye View

A major combat support agency of the Department of Defense and a member of the Intelligence Community, the National Geospatial-Intelligence Agency provides timely, relevant and accurate imagery, imagery intelligence and geospatial information in support of national security objectives. Headquartered in Bethesda, Md., NGA operates major facilities in the Washington, D.C., and St. Louis, Mo., areas and services a wide array of customers through liaisons and support teams stationed around the world.

OUR VISION:
KNOW THE EARTH...SHOW THE WAY

OUR CORE VALUES:
In NGA, we are committed to...
PARTNERS
Both as a National Intelligence and a Combat Support Agency
PEOPLE
Their personal integrity, professionalism, growth, leadership, and accountability
CULTURE
Our diversity, teamwork, creativity, risk-taking, and mutual trust and respect

...EXCELLENCE IN ALL WE DO

POINTS OF CONTACT

CWID Program Office (IIG)

NGA, Mail Stop P-127
12310 Sunrise Valley Drive
Reston, VA 20191



JOINT INTEROPERABILITY TEST COMMAND

Focusing on Interoperability

As tasked in Chairman of the Joint Chiefs of Staff Instruction 6260.01, JITC supports CWID in the following ways:

SENIOR MANAGEMENT GROUP (SMG)

JITC provides a non-voting representative to the CWID SMG to advise the SMG on interoperability issues and challenges.

ASESSMENT WORKING GROUP (AWG)

As Chairperson of the AWG, JITC ensures that assessments performed by the Technical, Warfighter Utility and Information Assurance Assessment Teams not only compliment each other, but provide an overall assessment of all aspects of a trial. The AWG Chair also interfaces directly with other CWID Working Groups and sites to coordinate on matters related to the assessment of the participating trials.

TECHNICAL ASESSMENT APROACH

In addition to chairing the AWG, JITC performs Technical Assessments. Throughout the CWID process, JITC works with each trial's representative to clearly define the data requirements and information exchanges associated with the capabilities that the trial will demonstrate during the CWID execution. These requirements focus on external interfaces, data exchanges between the trial and CWID core services, service component systems (GCCS, AFATDS, etc.) or other CWID Interoperability Trials. Details that are documented for each trial include: The hardware/software configuration, ports and/protocols used, data or media formats, the type of data being exchanged, the physical path that will be used to exchange the data and the anticipated results of the information exchanges. During the CWID Execution, JITC coordinates with each trial assessed to document results of data transfers and information exchanges, ensuring data transferred during the exchange is processed correctly by the receiving system.

INTEROPERABILITY RESULTS

Following execution, JITC analysts review the results of each trial's data transfers demonstrated during execution. JITC documents, in the WISE Interoperability Collection Assessment Tool (WICAT), the successes and any problems encountered during data transfers, and the ability of the end user to process the data exchanged. Once all results have been input and consolidated, JITC passes this information to the CWID Joint Management Office (JMO) in the form of a database that provides a "snapshot view" of the interoperability status of each trial assessed. In addition, JITC provides the CWID JMO a narrative summary of the trials's performance that further defines results of the information exchange, hardware and software configuration and connectivity to the network for inclusion in the CWID Final Report. All data that JITC collects on Information Technology (IT) and National Security System (NSS) trials during the CWID process can be carried forward and applied toward an Interoperability Certification.

CONTACT
Jeff Phipps
(301) 744-2883
(DSN) 354-2883
jeff.phipps@disa.mil

http://jitc.fhu.disa.mil

INFORMATION ASSURANCE

In its role as an Operational Test Agency (OTA) for the Director, Operational Test and Evaluation (DOT&E), JITC supports CWID by augmenting the NSA in the preparation and conduct of Information Assurance Assessments performed on selected ITs. If required, JITC can support the staff assigned to the National Information Assurance Team (NIAT) during CWID execution.